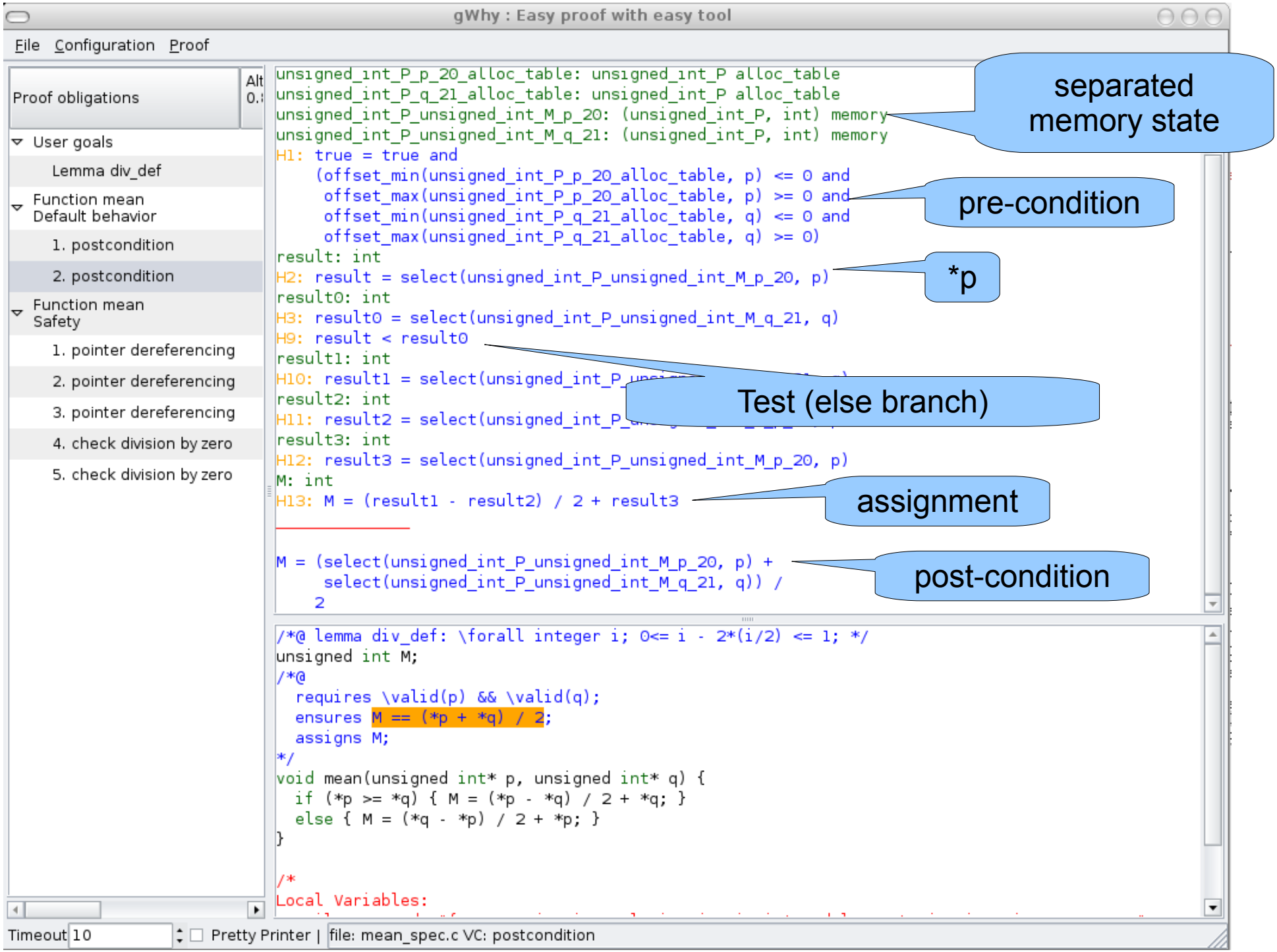
gWhy : Easy proof with easy tool
File Configuration Proof
Proof obligations
Alt 0.
User goals
Lemma div_def
Function mean Default behavior
1. postcondition
2. postcondition
Function mean Safety
1. pointer dereferencing
2. pointer dereferencing
3. pointer dereferencing
4. check division by zero
5. check division by zero
unsigned_int_P_p_20_alloc_table: unsigned_int_P alloc_table
unsigned_int_P_q_21_alloc_table: unsigned_int_P alloc_table
unsigned_int_P_unsigned_int_M_p_20: (unsigned_int_P, int) memory
unsigned_int_P_unsigned_int_M_q_21: (unsigned_int_P, int) memory
H1: true = true and
(offset_min(unsigned_int_P_p_20_alloc_table, p) <= 0 and
offset_max(unsigned_int_P_p_20_alloc_table, p) >= 0 and
offset_min(unsigned_int_P_q_21_alloc_table, q) <= 0 and
offset_max(unsigned_int_P_q_21_alloc_table, q) >= 0)
result: int
H2: result = select(unsigned_int_P_unsigned_int_M_p_20, p)
result0: int
H3: result0 = select(unsigned_int_P_unsigned_int_M_q_21, q)
H9: result < result0
result1: int
H10: result1 = select(unsigned_int_P
result2: int
H11: result2 = select(unsigned_int_P
result3: int
H12: result3 = select(unsigned_int_P_unsigned_int_M_p_20, p)
M: int
H13: M = (result1 - result2) / 2 + result3
M = (select(unsigned_int_P_unsigned_int_M_p_20, p) +
select(unsigned_int_P_unsigned_int_M_q_21, q)) /
2
/*@ lemma div_def: \forall integer i; 0<= i - 2*(i/2) <= 1; */
unsigned int M;
/*@
requires \valid(p) && \valid(q);
ensures M == (*p + *q) / 2;
assigns M;
*/
void mean(unsigned int* p, unsigned int* q) {
if (*p >= *q) { M = (*p - *q) / 2 + *q; }
else { M = (*q - *p) / 2 + *p; }
}
/*
Local Variables:
separated memory state
pre-condition
*p
Test (else branch)
assignment
post-condition
Timeout 10
Pretty Printer |
file: mean_spec.c VC: postcondition